SKT. JOSEF'S
ROSKILDE INTERNATIONAL SCHOOL

Privacy policy and guidelines for personal data usage and storaged at St. Josef's School

CONTENTS

Data controller at St. Josef's School

The person responsible, the data controller, at St. Josef's School is the school the leader/principal.

Data use agreements

Data usage agreements have been entered into with the school's data providers. Data usage agreements are stored in the GDPR folder.

Legislation and school policies
All employees of St. Josef's School must follow the applicable rules for the handling and storage of personal data, in accordance with EU General Data Protection Data Regulation (GDPR) of 25th May 2018.
The School of St. Josef has prepared:

- General policy and guidelines for the handling and retention of personal data at Skt. Josef's School (This policy)
- Policy for the storage and handling of personal data on pupils and parents
- ICT security policy for employees of St. Josef's School.

This policy specifies the rules that must be complied with, and how we, as a school, should take action in the event of a breach of data security.
The policies are available on the school website www.sktjosefs.com

Definition of personal data:

General Personal Data:
Name and address,
CPR Number
Photo
Salaries and taxes
Sick leave
Criminal record
Interests
Logging (electronic tracks)
Sensitive personal data:
Race and Ethnicity
Political and religious beliefs
Opinions affiliation
Health information
Biometric Data
Sexual beliefs
Social and private affairs

Manually stored data (paper archives, registers, etc., found in physical form)
Personal data – both common and sensitive must be stored in locked file cabinets.
The archives may only be available to employees who have a working need.
The archives must be stored in a safe place and must not be accessible to unauthorized persons.

Digital data (data recorded in ICT systems)
The employee's job function determines the data that can be accessed. It is the administrator of each system that assigns permissions to all employee groups. See Administrator Overview.

ICT-security policy for employees of St. Josef's School
The school has developed a separate ICT security policy for employees at St. Josef's School. All employees are made aware of the policy in relation to their employment. ICT policy covers home workstations, portable work computers, desktop computers, email management, social media, passwords, screen lock, etc.

Consent statements
A number of consent statements have been prepared for the storage and handling of personal data for pupils, parents and employees. The following declarations of consent are used:

Students
Consent-student and parent personal data
Consent-for special additional information
Consent-additional relationships
Consent- to obtain information from kindergarten
Consent- to obtaining information from current or previous school

In addition, upon entry to the waiting list on the website of the school, consent is given to allow the school to keep personal data for pupils who are registered on a waiting list.

Employees
Consent-collection, storage and handling of employee personal data.

Photos of pupils and employees
Parents and employees must consent to the school's keeping and using portrait images.
Consent is part of the general declaration of consent as parents and employees give by joining and hiring respectively.

Personal data in Skoleintra
Skoleintra is a cooperation platform between school, students and parents. If you have a protected address, the address information will not be transferred to Skoleintra. As a parent, if you do not want this information to be shown in lists etc. you must change this yourself in Forældreintra under Settings.
Concent for keeping data is obtained through the general consent form.

Student and parent portals
Data agreements have been acquired from suppliers of pupil and parent portals. See section in GDPR folder.

Learning portals and platforms
Data agreements have been concluded with providers of learning portals and platforms. See section in GDPR folder.

Disclosure of sensitive information to third parties
Information may be disclosed to third parties only after written consent of the parents for the collection and disclosure of sensitive personal data. In such cases, custody holders must sign the consent form for obtaining additional sensitive information.

Disposal of Digital Data
The disposal of digital data on pupils, parents and employees is subject to applicable law.
See Storage and Data Disposal overview.

Disposal of physical archives
The disposal of physical archives by pupils, parents and employees is subject to applicable law.

Physical material will be shredded. Materials will be kept in a locked cabinet until shredding can take place.

Access to School
All employees have access on weekdays between 7.00 – 17.00. Outside this time, electronic access keys must be used.
The password for disarming the security alarm to the administration and management area is also required outside the above-mentioned period.

Breach of data security
In the event of a breach of data security, the management/controller shall be informed immediately. The management and the controller shall then assess the further progress, including reporting to the data Applicable rules on the website of the Data Protection Authority.

31 of March 2020/BP